J. Symbolic Computation (1992) **14**, 483–503

Gröbner Bases and Primary Decomposition of Modules

ELIZABETH W. RUTMAN†

University of Maryland
: Rutgers University

(*Received* 27 *April* 1992)

In this paper I present definitions and algorithms for Gröbner bases for submodules of free modules over polynomial rings in n variables over Noetherian commutative rings with certain algorithmic properties. I then give an algorithm for computing the primary decomposition of submodules of submodules of these free modules when the base ring is also a PID, and show that under certain dimension conditions the requirement of a PID may be dropped.

1. Introduction

In this paper I present an algorithm for computing the primary decomposition of a submodule of a submodule of a free module of a polynomial ring in n variables. The base ring R must be a PID in which ideal membership is decidable and syzygies are computable, and in which we are given an algorithm for factoring polynomials over fields which are finitely generated over R or are residue fields of R. Examples of such rings are the integers $\mathbf{Z}$, the rational numbers $\mathbf{Q}$, and finite fields.

There has been a lot of recent work done to compute primary decompositions for ideals in polynomial rings. Most of the algorithmic techniques rely on the computability of Gröbner bases, which were first constructed by Buchberger (1985). Lazard (1985) gives an explicit structure theorem for the Gröbner basis of an ideal in a polynomial ring in two variables over a field. From this he gives an algorithm for constructing a Gröbner basis for each primary component of a zero-dimensional ideal. Gianni, Trager, and Zacharias (1988) give an algorithm for computing the primary decomposition of an ideal in a polynomial ring in n variables over a principal ideal domain (PID). The restriction to a PID is removable if certain other conditions exist.

Möller (1988) generalizes Buchberger's algorithm to include ideals in polynomial rings over more general rings R in which certain conditions about computability exist. Möller and Mora (1986) generalize the notion of Gröbner bases to submodules of free modules of polynomial rings over a field.

My construction of a primary decomposition for a module relies on the work done by Gianni, Trager and Zacharias (1988). In the next section, I define the basic notation I will use, and discuss the types of rings I will allow. The third section generalizes the Gröbner basis definitions and properties of (Möller, 1988, section 2) to modules. The

0747-7171/92/110483+21 $08.00/0

fourth section shows how, just as in (Gianni, Trager and Zacharias, 1988) for ideals, many module operations can be effectively computed using Gröbner bases. I then, in the next two sections, give a basic overview of primary modules and the dimension of modules, and show how Gröbner bases can be related to both of these algebraic notions. Section 7 gives an algorithm for the special case of a zero-dimensional module and R is not necessarily a PID, and section 8 gives the algorithm for the case when R is a PID.

2. Some Notation

Let R be a Noetherian commutative ring with identity. If M is any R-module generated by a set $V = \{v_1, \ldots, v_m\} \subset M$, we will write $M = \langle v_1, , \ldots, , v_m \rangle$. We say that M is *given* if we are given a finite set of generators for M. We will use the following standard notation. If $S \subseteq R$ is a multiplicatively closed set, $I \subset R$ is an ideal of R, $\wp \subset R$ is a prime ideal of R, N and M are R-modules, and $f \in R$, then we define

$\mathrm{N} = \{0, 1, 2, 3, \ldots\}$	the non-negative integers
$\sqrt{I} = \{a \mid a^m \in I \text{ for some } m \in \mathrm{N}\}$	the radical of I
$S^{-1}M = \{\frac{m}{s} \mid s \in S, m \in M\}$	the localization of M at S
$M_\wp = S^{-1}M$ where $S = R - \wp$	the localization of M at $\wp$
$M_f = S^{-1}M$ where $S = \{f^m \mid m \in \mathrm{N}\}$	the localization of M at f
$Ann_R(M) = \{r \in R \mid rM = 0\}$	the annihilator of M
$N : M = \{r \in R \mid rM \subseteq N\}$	the quotient of M by N.

We note the following:

1. If it is clear which ring R we are in, we will write $Ann(M)$ for $Ann_R(M)$;
2. If $N \subseteq M$ then $N : M = Ann(M/N)$;
3. If $M \subseteq R^t$ then $M_\wp = MR_\wp$, the submodule of the ring $R_\wp^t$ generated by M.

DEFINITION 2.1. We say that *linear equations are solvable in* R if:

(i) Given $a, a_1, \ldots, a_m \in R$ it is possible to decide if $a \in \langle a_1, \ldots, a_m \rangle$ and, if so, find $b_1, \ldots, b_m \in R$ such that $a = \sum b_i a_i$.
(ii) Given $a_1, , \ldots, , a_m \in R$ it is possible to find a finite set of generators for the R–module $\{(b_1, , \ldots, , b_m) \mid \sum b_i a_i = 0\}$.

In other words, ideal membership and syzygy modules are effectively computable in R . From now on we will always assume that R is a Noetherian commutative ring with identity in which linear equations are solvable.

3. Gröbner Bases for Modules

In this section we generalize the results in (Möller, 1988, section 2) to submodules of free modules over R. Theorem 3.6 and its proof are the module analog of (Möller, 1988, theorem 1). These results show Gröbner bases exist and are effectively computable for modules.

Given $n \in \mathrm{N}$ and a set of indeterminates $x_1, \ldots, x_n$, we define the set of power products of the polynomial ring $R[x_1, \ldots, x_n] = R[X]$ by

$$T = \{X^\alpha = {x_1}^{\alpha_1} \cdots {x_n}^{\alpha_n} \mid \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathrm{N}^n\}.$$

Let us assume we are given a term order $<$ on T. For any $f \in R[X]$ we may write $f = \sum_{i=1}^{r} c_i X^{\alpha_i}$ with $c_i \in R - \{0\}$ and $\alpha_i \in \mathbf{N}^n$, and $\alpha_r < \cdots < \alpha_1$. With this notation we define $lc(f) = c_1$, the leading coefficient of f; $lp(f) = X^{\alpha_1}$, the leading power product of f; $lt(f) = c_1 X^{\alpha_1}$, the leading term of f.

For some positive integer s, we now consider $R[X]^s$. The set of terms of $R[X]^s$ is defined to be

$$T_s = \{(\varphi_1, \ldots, \varphi_s) \mid \exists i \in \{1, \ldots, s\} \text{ such that } \varphi_i \in T \text{ and } \varphi_j = 0 \ \forall j \neq i\}.$$

Using the standard unit basis vectors $\{e_1, \ldots, e_s\}$ in $R[X]^s$, we may write $T_s = \bigcup_{i=1}^{s} Te_i$ (disjoint) where $Te_i = \{\varphi e_i \mid \varphi \in T\}$. Given a term order $<_T$ on T there are a number of ways we can extend this to a term order on T_s, but only two such orders will be of importance to us. The first, which we will call TOP and denote by $<_{TOP}$, regards the term order of the coordinates more highly than their position in the vector. Given $\Phi = \varphi e_i$ and $\Psi = \psi e_j$ in T_s, with $\varphi, \psi \in T$, we define

$$\Phi <_{TOP} \Psi \iff \begin{array}{ll} \text{either} & \varphi <_T \psi \\ \text{or} & \varphi = \psi \text{ and } j < i. \end{array}$$

The second, which we call POT and denote by $<_{POT}$, regards the position of the coordinates in the vector more highly than their term orders. Thus we define

$$\Phi <_{POT} \Psi \iff \begin{array}{ll} \text{either} & j < i \\ \text{or} & j = i \text{ and } \varphi <_T \psi. \end{array}$$

When it is clear which order we are using, or when the order is arbitrary, we may drop the subscript and simply write $<$. We note that these term orders on T_s induced by a term order $<_T$ on T have the properties that $\Phi < \Psi \Rightarrow \varphi\Phi < \varphi\Psi \ \forall \varphi \in T$ and $\forall \Phi, \Psi \in T_s$; and $\varphi <_T \psi \Rightarrow \varphi\Phi < \psi\Phi \ \forall \varphi, \psi \in T$ and $\forall \Phi \in T_s$. As above for $R[X]$, for any $F \in R[X]^s$ we may write $F = \sum_{i=1}^{r} c_i \Phi_i$ with $c_i \in R - \{0\}$, $\Phi_i \in T_s$, and $\Phi_r < \cdots < \Phi_1$. We then define $lc(F) = c_1$, the leading coefficient of F; $lp(F) = \Phi_1$, the leading power product of F; $lt(F) = c_1\Phi_1$, the leading term of F. For any subset $\Omega \subseteq R[X]^s$ we define the leading term module of Ω by $Lt(\Omega) = \langle \{lt(F) \mid F \in \Omega\} \rangle$.

Definition 3.1. Given an $R[X]$-module $N \subseteq R[X]^s$, a subset $\Omega \subseteq N$ is a *Gröbner basis* for N if $Lt(\Omega) = Lt(N)$.

When $s = 1$, this definition for Gröbner bases is the one given by (Gianni, Trager and Zacharias, 1988) for ideals. Möller (1988) uses this definition for what he calls "weak Gröbner bases".

Definition 3.2. Given an $R[X]$-module $N = \langle G_1, \ldots, G_m \rangle \subseteq R[X]^s$ and an element $F \in N$, $\exists v_1, \ldots, v_m \in R[X]$ such that $F = \sum v_i G_i$. We call this a *Gröbner representation of* F (in terms of $G_1, \ldots, G_m$) if $lp(F) = \max_i \{lp(v_i) lp(G_i)\}$.

Definition 3.3. Let $\Omega = \{G_1, \ldots, G_m\} \subset R[X]^s$ and $F, H \in R[X]^s$. We say that F *reduces to* H *modulo* Ω, written $F \rightarrow_\Omega H$, if $lp(H) < lp(F)$ and $F - H$ has a Gröbner representation in terms of Ω. We define $\rightarrow_\Omega^+$ to be the reflexive transitive closure of $\rightarrow_\Omega$. If no $H \neq F$ exists such that $F \rightarrow_\Omega^+ H$ we say F is *reduced modulo* Ω.

Note that the reduction $\rightarrow_\Omega^+$ is Noetherian, i.e. there is no infinite sequence $F_1 \rightarrow_\Omega^+$

$F_2 \to_\Omega^+ \cdots$. The proof is the same as in the ideal case (see Gianni, Trager and Zacharias, 1988). Moreover, a reduction algorithm exists which, given F and Ω, computes H such that H is reduced and $F \to_\Omega^+ H$. This algorithm is the same as that for ideals.

DEFINITION 3.4. For $F_1, \ldots, F_r \in R[X]^s$, let $B = (lt(F_1), \ldots, lt(F_r))$. We say that $G = (g_1, \ldots, g_r) \in R[X]^r$ is a *syzygy with respect to* B if $\sum_{i=1}^r g_i lt(F_i) = 0$. We say G is *homogeneous* if for some $\Phi \in T_s$ we have either $g_i = 0$ or $g_i = lt(g_i)$ and $lp(g_i)lp(F_i) = \Phi$ for $i = 1, \ldots, r$. We call Φ the *degree* of G.

The set $S(B)$ of all syzygies with respect to a given tuple B is called the module of syzygies with respect to B .

LEMMA 3.5. *$S(B)$ is a homogeneous module (i.e. any $G \in S(B)$ splits into a sum of homogeneous r-tuples, all of which are also in $S(B)$)* .

PROOF. Suppose $B = (lt(F_1), \ldots, lt(F_r))$ with $F_j \in R[X]^s$ for $j = 1, \ldots, r$, and suppose $G = (g_1, \ldots, g_r) \in S(B)$. Let $\{e_1, \ldots, e_s\}$ and $\{e'_1, \ldots, e'_r\}$ be the standard unit basis vectors for $R[X]^s$ and $R[X]^r$ respectively. For $j = 1, \ldots, r$, write $lt(F_j) = lt(f_j)e_{\sigma(j)}$ for some $f_j \in R[X]$ and $\sigma(j) \in \{1, \ldots, s\}$. For each $i \in \{1, \ldots, s\}$ let $J_i = \{j \mid \sigma(j) = i\}$, and notice that $\{1, \ldots, r\} = \bigcup_{i=1}^s J_i$ (disjoint). Since

$$0 = \sum_{j=1}^r g_j lt(F_j) = \sum_{i=1}^s \sum_{j \in J_i} g_j lt(F_j) = \sum_{i=1}^s \sum_{j \in J_i} g_j lt(f_j) e_i$$

then for each i $\sum_{j \in J_i} g_j lt(f_j)e_i = \sum_{j \in J_i} g_j lt(F_j) = 0$. Let $G_i = \sum_{j \in J_i} g_j e'_j$. Then $G = \sum_{i=1}^s G_i$ and each $G_i \in S(B)$. Moreover, $G_i \in S(B_i)$ where $B_i = \sum_{j \in J_i} lt(f_j)e'_j$.

Now, if we can write $G_i = \sum_k H_{ik}$ with each $H_{ik} \in S(B_i)$ homogeneous of degree $\phi_{ik} \in T$ and such that $H_{ik} = \sum_{l=1}^r h_{ikl}e'_l$ with $h_{ikl} = 0 \ \forall l \notin J_i$, then setting $\Phi_{ik} = \phi_{ik}e_i$ we see that $H_{ik} \in S(B)$ and is homogeneous of degree $\Phi_{ik} \in T_s$. We have thus reduced the proof to the case where $s = 1$.

Thus it suffices to show that if $B = (lt(f_1), \ldots, lt(f_r))$ with $f_i \in R[X]$, and $H = (h_1, \ldots, h_r) \in S(B)$, then H splits into a sum of homogeneous syzygies of B . (Note that this is not necessarily the same r as above.) Let us write $h_i = \sum_{j=1}^{t_i} a_{ij}\psi_{ij}$, with ψ_{ij} distinct elements of T and $a_{ij} \in R$. We then have that

$$\sum_{i=1}^r h_i lt(f_i) = \sum_{i=1}^r \sum_{j=1}^{t_i} a_{ij}\psi_{ij} lt(f_i) = 0.$$

Let $J_{ij} = \{\psi_{\alpha\beta} \mid \psi_{\alpha\beta} lp(f_\alpha) = \psi_{ij} lp(f_i)\}$, and notice that for any two pairs (i, j) and (α, β) either $J_{ij} = J_{\alpha\beta}$ or $J_{ij} \cap J_{\alpha\beta} = \emptyset$. Moreover, since we assumed that the ψ_{ij}'s are all distinct, if $\psi_{\alpha\beta} \in J_{ij}$ then $\psi_{\alpha\gamma} \notin J_{ij}$ $\forall \gamma \neq \beta$. Let Λ be a set of representative pairs (i, j) for the distinct sets J_{ij}, and for each $(i, j) \in \Lambda$ let

$$H_{ij} = \sum_{(\alpha,\beta) \in J_{ij}} a_{\alpha\beta}\psi_{\alpha\beta}e'_\alpha.$$

By construction, $\sum_{(\alpha,\beta) \in J_{ij}} a_{\alpha\beta}\psi_{\alpha\beta} lt(f_\alpha) = 0$, hence $H_{ij} \in S(B)$. Moreover, H_{ij} is homogeneous of degree $\psi_{ij} lp(f_i)$ and $H = \sum_{(i,j) \in \Lambda} H_{ij}$. □

THEOREM 3.6. *Let* $\Omega = \{G_1, \ldots, G_r\} \subset R[X]^s$. *Let* $N = \langle G_1, \ldots, G_r \rangle$, *and* $B = (lt(G_1), \ldots, lt(G_r))$. *Then the following are equivalent:*

(i) Ω *is a Gröbner basis for* N.
(ii) *Every* $F \in N$ *has a Gröbner representation in terms of* Ω.
(iii) *If* $H_1, \ldots, H_m$ *is a basis for* $S(B)$, *with* $H_i = (h_{i1}, \ldots, h_{ir})$ *homogeneous of degree* Φ_i *for* $i = 1, \ldots, m$, *then every S-polynomial* $S(H_i, \Omega) = \sum_{j=1}^{r} h_{ij} G_j$ *has a Gröbner representation in terms of* Ω.
(iv) $F \to_{\Omega}^{+} 0$ *for all* $F \in N$.
(v) *If* $H_1, \ldots, H_t$ *is any basis for* $S(B)$, *then* $S(H_i, \Omega) \to_{\Omega}^{+} 0$ *for* $i = 1, \ldots, t$.

PROOF. (i) $\Rightarrow$ (ii) Let $F \in N$, and suppose, by induction on the well-ordering of the term order, that a Gröbner representation already exists for all $H \in N$ with $lp(H) < lp(F)$. By (i) we have $lt(F) = \sum_{i=1}^{r} h_i lt(G_i)$, with $h_i \in R[X]$, $i = 1, \ldots, r$. Without loss of generality we may assume for each i either $h_i = 0$ or $lp(h_i)lp(G_i) = lp(F)$ for $i = 1, \ldots, r$. Let $F_1 = F - \sum h_i G_i$. By construction, the leading term of $\sum h_i G_i$ cancels the leading term of F, thus $lp(F_1) < lp(F)$. Hence we have a Gröbner representation for F_1 in terms of Ω, say $F_1 = \sum_{i=1}^{r} g_i G_i$, with $lp(g_i)lp(G_i) \leq lp(F_1) < lp(F)$ for each i. Writing $F = \sum (g_i + h_i) G_i$ we see that this is indeed a Gröbner representation for F in terms of Ω.

(ii) $\Rightarrow$ (iii) This is clear since each S-polynomial is in N .

(iii) $\Rightarrow$ (i) It suffices to show that for any $F \in N$, $lt(F) \in Lt(\Omega)$. Let $\{e'_1, \ldots, e'_r\}$ be the standard unit basis for $R[X]^r$. Consider an arbitrary representation $F = \sum_{i=1}^{r} u_i G_i$. Let $\Phi = \max_i \{lp(u_i)lp(G_i)\}$ and $J = \{j \mid lp(u_j)lp(G_j) = \Phi\}$. If $lp(F) = \Phi$ then $lt(F) = \sum_{j \in J} lt(u_j)lt(G_j)$, and hence $lt(F) \in Lt(\Omega)$. Otherwise, $lp(F) < \Phi$. In this case $\sum_{j \in J} lt(u_j)lt(G_j) = 0$, and so $H = \sum_{j \in J} lt(u_j) e'_j \in S(B)$. Moreover, H is homogeneous of degree Φ. Since $H \in S(B)$ we have $H = \sum_{i=1}^{m} g_i H_i$ for some $g_1, \ldots, g_m \in R[X]$. We may assume that for each i either $g_i = 0$ or $lp(g_i)\Phi_i = \Phi$. To see this, write $g_i = \sum_{\nu \in \mathbf{N}^n} c_{i\nu} X^{\nu}$ for some $c_{i\nu} \in R$, only finitely many of which are nonzero. Then

$$\sum_{j \in J} lt(u_j) e'_j = H = \sum_{\nu \in \mathbf{N}^n} \sum_{i=1}^{m} c_{i\nu} X^{\nu} H_i = \sum_{j=1}^{r} \Big(\sum_{i,\nu} c_{i\nu} X^{\nu} h_{ij} \Big) e'_j .$$

Recall that for each i and j either $h_{ij} = 0$ or $h_{ij} = lt(h_{ij})$ and $lp(h_{ij})lp(G_j) = \Phi_i$. Fix j. Then

$$\sum_{i,\nu} c_{i\nu} X^{\nu} h_{ij} = \sum_{\Psi \in T,} \Big(\sum_{X^{\nu}\Phi_i = \Psi} c_{i\nu} X^{\nu} h_{ij} \Big) = \begin{cases} lt(u_j) & \text{if } j \in J \\ 0 & \text{if } j \notin J. \end{cases}$$

Thus, if $X^{\nu}\Phi_i \neq \Phi$, we see that we may take $c_{i\nu} = 0$. Then

$$g_i = \sum_{\{\nu \mid X^{\nu}\Phi_i = \Phi\}} c_{i\nu} X^{\nu},$$

hence now either $g_i = 0$ or $lp(g_i)\Phi_i = \Phi$. Also, by (iii) we have the Gröbner representations $S(H_i, \Omega) = \sum_{j=1}^{m} h_{ij} G_j = \sum_{j=1}^{m} v_{ij} G_j$ with $lp(v_{ij})lp(G_j) < \Phi_i$. The inequality comes from $\max_j \{lp(v_{ij})lp(G_j)\} = lp(\sum_{j=1}^{r} h_{ij} G_j)$ and the right hand side is less than

Φ_i since H_i is homogeneous of degree Φ_i and is in $S(B)$. Thus we have

$$\sum_{j\in J} lt(u_j)G_j = \sum_{i=1}^{r} g_i \sum_{j=1}^{m} h_{ij}G_j = \sum_{j=1}^{m}\sum_{i=1}^{r} g_i h_{ij} e_j.$$

The maximal term on the left hand side is Φ, on the right hand side $< \Phi$. Thus, replacing the left hand side with the right hand side in the equation $F = \sum_{i=1}^{m} u_i G_i$, we obtain a representation for F with maximal term $< \Phi$. Iterating this procedure, we obtain a Gröbner representation for F which, as seen above, shows $lt(F) \in Lt(\Omega)$.

(i) $\Rightarrow$ (iv) Let $F \in N$, and suppose by induction that $H \to_\Omega^+ 0$ for all $H \in N$ with $lp(H) < lp(F)$. Since $F \in N$ we have by (i) that $lt(F) = \sum_{i=1}^{r} h_i lt(G_i)$. Without loss of generality we may assume that for each i either $h_i = 0$ or $lp(h_i)lp(G_i) = lp(F)$. Let $F_1 = F - \sum_{i=1}^{r} h_i G_i$. Then $F \to_\Omega F_1$ and, by assumption since $lp(F_1) < lp(F)$, $F_1 \to_\Omega^+ 0$. Thus, by transitivity of $\to_\Omega^+$, $F \to_\Omega^+ 0$.

(iv) $\Rightarrow$ (v) This is clear since all S-polynomials are in N .

(v) $\Rightarrow$ (iii) Suppose we have $S(H_i, \Omega) = \sum_{j=1}^{r} h_{ij}G_j = F_0 \to_\Omega F_1 \to_\Omega \cdots \to_\Omega F_l = 0$. Summing up the Gröbner representations of each of $F_{i-1} - F_i$ for $i = 1, \ldots, l$ we get a Gröbner representation of F_0. □

REMARK. Notice that the proof of (i) $\Rightarrow$ (ii) did not make use of the fact that $N = \langle G_1, \ldots, G_r \rangle$. Thus we have shown that if Ω is a Gröbner basis for N then $N = \langle \Omega \rangle$.

THEOREM 3.7. *Let $<$ be a term order on $R[X]^s$ and let N be a submodule of $R[X]^s$. Then there exists a Gröbner basis for N . Moreover, such a Gröbner basis is effectively computable in a finite number of steps.*

PROOF. As a result of Theorem 3.6, the usual Buchberger algorithm can be modified to compute a Gröbner bases for N (see Buchberger, 1985). □

Note: CoCoA currently computes Gröbner bases for modules when R is a field, using either the TOP or POT order on T_s.

4. Operations on Modules

Using Gröbner bases many operations on modules are effectively computable. All of the results of this section generalize results of (Gianni, Trager and Zacharias, 1988, Section 3) to the case of submodules of free modules of $R[X]$, and we will only refer to the results of (Gianni, Trager and Zacharias, 1988) for the ideal cases.

Let $N \subseteq R[Y, X]^s = R[y_1, \ldots, y_m, x_1, \ldots, x_n]^s$ be a module, and suppose we are given two orders $<_x$ and $<_y$ on monomials of $R[Y, X]$ in X and Y respectively. We define a term order $<$ on $R[Y, X]$ by

$$X^{\alpha_1}Y^{\beta_1} < X^{\alpha_2}Y^{\beta_2} \iff \begin{array}{ll} \text{either} & X^{\alpha_1} <_x X^{\alpha_2} \\ \text{or} & X^{\alpha_1} = X^{\alpha_2} \text{ and } Y^{\beta_1} <_y Y^{\beta 2}. \end{array}$$

$\forall \alpha_1, \alpha_2 \in \mathbf{N}^n$ and $\forall \beta_1, \beta_2 \in \mathbf{N}^m$. Notice that this is a lexicographical ordering between X and Y (and is often called an elimination order).

PROPOSITION 4.1. *(i) If $\prec_x$, $\prec_y$, and $\prec$ are the corresponding POT term orders on*

$R[Y,X]^s$ and Ω is a Gröbner basis for N with respect to $\prec$, then Ω is a Gröbner basis for $N \subseteq (R[Y])[X]^s$ with respect to $\prec_x$.
(ii) If $\prec_x$, $\prec_y$, and $\prec$ are the corresponding TOP term orders on $R[Y,X]^s$ and Ω is a Gröbner basis for N with respect to $\prec$, then $\Omega \cap R[Y]^s$ is a Gröbner basis for $N \cap R[Y]^s \subseteq R[Y]^s$ with respect to $\prec_y$.

PROOF. (i) We wish to show $Lt_{\prec_x}(\Omega) = Lt_{\prec_x}(\langle\Omega\rangle)$.
$\subseteq$: Clear.
$\supseteq$: Let $\{e_1,\ldots,e_s\}$ be the standard unit basis vectors for $R[X,Y]^s$. Let $F \in N$, and suppose $\Omega = \{G_1,\ldots,G_r\}$. Since Ω is a Gröbner basis for N, we can write $F = \sum_{j=1}^{t} c_j Y^{\nu_j} X^{\mu_j} G_{i_j}$, where $c_j \in R$, such that

$$Y^{\nu_1}X^{\mu_1} lp_{\prec}(G_{i_1}) \geq Y^{\nu_2}X^{\mu_2} lp_{\prec}(G_{i_2}) \geq \cdots \geq Y^{\nu_r}X^{\mu_r} lp_{\prec}(G_{i_t})$$

and $lp_{\prec}(F) = Y^{\nu_1}X^{\mu_1} lp_{\prec}(G_{i_1})$. Then $\exists t_o$ such that

$$Y^{\nu_1}X^{\mu_1} lp_{\prec}(G_{i_1}) = \cdots = Y^{\nu_{t_0}}X^{\mu_{t_0}} lp_{\prec}(G_{i_{t_0}}) > Y^{\nu_{t_0+1}}X^{\mu_{t_0+1}} lp_{\prec}(G_{i_{t_0+1}}).$$

Write

$$G_{i_j} = a_{i_j}(Y)X^{\beta_{i_j}} e_{\sigma(i_j)} + \text{ lower X-terms with respect to } \prec_x$$

and notice that $\{X^{\mu_{i_j}+\beta_{i_j}} e_{\sigma(i_j)}\}$ is a decreasing sequence in $R[Y,X]^s$. (Here the fact that we are using POT is crucial.) Then $\exists t_1 \geq t_0$ such that

$$X^{\mu_1+\beta_{i_1}} e_{\sigma(i_1)} = \cdots = X^{\mu_{t_1}+\beta_{i_{t_1}}} e_{\sigma(i_{t_1})} > X^{\mu_{t_1+1}+\beta_{i_{t_1+1}}} e_{\sigma(i_{t_1+1})}.$$

Thus

$$\begin{aligned} lt_{\prec_x}(F) &= \sum_{j=1}^{t_1} c_j Y^{\nu_j} X^{\mu_j} a_{i_j}(Y) X^{\beta_{i_j}} \\ &= \underbrace{\left(\sum_{j=1}^{t_1} c_j Y^{\nu_j} a_{i_j}(Y)\right)}_{(*)} X^{\mu_j+\beta_{i_j}} \\ &= \sum_{j=1}^{t_1} c_j Y^{\nu_j} X^{\mu_j} lt_{\prec_x}(G_{i_j}) \end{aligned}$$

as long as $(*) \neq 0$. However,

$$lt_{\prec_y}(*) = lt_{\prec_y}\Big(\sum_{j=1}^{t_1} c_j Y^{\nu_j} a_{i_j}(Y)\Big) = \sum_{j=1}^{t_0} c_j Y^{\nu_j} lt_{\prec_y}(a_{i_j}(Y)) = \frac{lt_{\prec}(F)}{X^{\mu_1+\beta_{i_1}}} \neq 0.$$

Thus $lt_{\prec_x}(F) \in Lt_{\prec_x}(\Omega)$.
(ii) Notice that because of the TOP ordering, if $F \in R[Y,X]^s$ then $lt_{\prec}(F) \in R[Y]^s \iff F \in R[Y]^s$. Thus we have

$$Lt_{\prec}(\Omega \cap R[Y]^s) = Lt_{\prec}(\Omega) \cap R[Y]^s = Lt_{\prec}(N) \cap R[Y]^s = Lt_{\prec}(N \cap R[Y]^s).$$

So $\Omega \cap R[Y]^s$ is a Gröbner basis for $N \cap R[Y]^s$ with respect to $\prec$. But on $R[Y]^s$, $\prec$ coincides with $\prec_y$. □

REMARKS. We could not have switched the TOP and POT orders in the previous proposition. Part (i) is false if we use TOP instead. For example, if $\Omega = \{(x^2, 0), (x, xy)\} \subset \mathbf{Q}[y, x]^2$ then $lt_{\prec}(x^2, 0) = (x^2, 0)$ and $lt_{\prec}(x, xy) = (0, xy)$ and so, by Theorem 3.6 (v), Ω is a Gröbner basis for $\langle\Omega\rangle$. Let $G = (x^2, 0) - x(x, xy) = (0, x^2y)$. Then $lt(G) = (0, x^2y) \in Lt(\langle\Omega\rangle)$. However, $lt_{\prec_x}(x^2, 0) = (x^2, 0)$ and $lt_{\prec_x}(x, xy) = (x, 0)$, hence $lt(G) \notin Lt(\Omega)$. Thus Ω is not a Gröbner basis for $\langle\Omega\rangle$ with respect to $\prec_\alpha$. Also, part (ii) is false if we use POT instead. For example, if $\Omega = \{(y, x), (0, xy)\} \subset \mathbf{Q}[y, x]^2$ then $lt_{\prec}(y, x) = (y, 0)$ and $lt_{\prec}(0, xy) = (0, xy)$, and, again by Theorem 3.6 (v), Ω is a Gröbner basis for $\langle\Omega\rangle$. However, $(y^2, 0) = y(y, x) - (0, xy) \in \langle\Omega\rangle \cap \mathbf{Q}[y]^2$ while $\Omega \cap \mathbf{Q}[y]^2 = \emptyset$. Thus $\Omega \cap \mathbf{Q}[y]^2$ is not a Gröbner basis for $\langle\Omega\rangle \cap \mathbf{Q}[y]^2$ with respect to $\prec_y$.

COROLLARY 4.2. *Let M and N be given submodules of $R[X]^s$. Then the following can be effectively computed (i.e. a Gröbner basis can be found):*

(i) $M \cap N$
(ii) $N : M$
(iii) $M \cap N_f$, *where* $f \in R[X]$.

PROOF. (i) As in the case of ideals, we have

$$M \cap N = (zN + (z-1)M)R[X, z] \cap R[X]^s \tag{4.1}$$

where z is any other indeterminate, and the right hand side of 4.1 is computable using Proposition 4.1.

(ii) The proof is the same as that for ideals (see Gianni, Trager and Zacharias, 1988, Cor. 3.2(ii)).

(iii) Note that

$$M \cap N_f = (NR[X, z] + (zf - 1)R[X, z]^s) \cap M \tag{4.2}$$

where z is any other indeterminate, and the right hand side of 4.2 is computable using Proposition 4.1. □

PROPOSITION 4.3. *Let $S \subset R$ be a multiplicatively closed subset, $N \subseteq R[X]^s$ a submodule, and Ω a Gröbner basis for N . Then Ω is a Gröbner basis for $S^{-1}N \subset (S^{-1}R)[X]^s$.*

PROOF. $Lt(S^{-1}N) = S^{-1}Lt(N) = S^{-1}Lt(\Omega)$. That is, the leading terms of elements of Ω generate $Lt(S^{-1}N)$ in $S^{-1}R[X]^s$. □

LEMMA 4.4. *Let $V \subset S$ be multiplicatively closed subsets of R , and let $N \subseteq R[X]^s$ be a submodule. If*

$$S^{-1}Lt(N) \cap R[X]^s = V^{-1}Lt(N) \cap R[X]^s$$

then

$$S^{-1}N \cap R[X]^s = V^{-1}N \cap R[X]^s.$$

PROOF. Same as for ideals (see Gianni, Trager and Zacharias, 1988, Lemma 3.5). □

COROLLARY 4.5. *Let $S \subset R$ be a multiplicatively closed set and $N \subseteq R[X]^s$ a submodule. If $\exists a \in S$ such that*

$$S^{-1}Lt(N) \cap R[X]^s = (Lt(N)R_a[X]) \cap R[X]^s$$

then

$$S^{-1}N \cap R[X]^s = NR_a[X] \cap R[X]^s.$$

PROOF. Apply Lemma 4.4 with $V = \{a^m\}$. □

PROPOSITION 4.6. *Let R be an integral domain, $\wp = \langle p \rangle \subseteq R$ a principle prime ideal, and $N \subseteq R[X]^s$ a submodule. Then we can find $a \in R - \wp$ such that $NR_\wp[X] \cap R[X]^s = NR_a[X] \cap R[X]^s$. In particular, $NR_\wp[X] \cap R[X]^s$ can be computed.*

PROOF. Same as for ideals (see Gianni, Trager and Zacharias, 1988, Prop. 3.7). □

COROLLARY 4.7. *Let R be an integral domain, $\wp = \langle p \rangle \subseteq R$ a principle prime ideal, and $N \subset M$ submodules of $R[X]^s$. Then we can find $a \in R - \wp$ such that $NR_\wp[X] \cap M = NR_a[X] \cap M$.*

5. Primary Modules

For a complete treatment of primary ideals, we refer to (Zariski and Samuel, 1975, or Hungerford, 1974). Let R be a Noetherian commutative ring. For R-modules $N \subset M$, we say N is a *primary submodule of* M if whenever $r \in R, v \in M$ and $rv \in N$, either $v \in N$ or $r \in \sqrt{Ann(M/N)}$. In this case we see that $Ann(M/N)$ is a primary ideal of R, and if $\wp = \sqrt{Ann(M/N)}$ then $\wp$ is prime, and we say N is *$\wp$-primary in M*.

LEMMA 5.1. *Let $N \subset M$ be R-modules. If $\wp$ is a maximal ideal of R then N is $\wp$-primary in $M \iff Ann(M/N)$ is a $\wp$-primary ideal.*

PROOF. $\Rightarrow$: This follows from the remarks above.
$\Leftarrow$: Suppose $a \in R$, $v \in M$, and $av \in N$, and suppose $a \notin \sqrt{Ann(M/N)}$. Since $\sqrt{Ann(M/N)}$ is maximal, $\langle a, \sqrt{Ann(M/N)} \rangle = R$. Hence $\exists r \in R, \alpha \in \sqrt{Ann(M/N)}$ such that $1 = ra + \alpha$. Now $\alpha^m \in Ann(M/N)$ for some $m > 0$, so $1 = r'a + \alpha^m$, and hence $v = r'av + \alpha^m v \in N$. □

LEMMA 5.2. *Let R and S be rings and $\phi : R \to S$ a homomorphism. Let $N \subset M$ be S-modules with N $\wp$-primary in M. Then as R-modules, N is P-primary in M, where $P = \{r \in R \mid \phi(r) \in \wp\}$.*

PROOF. We note that clearly P is a prime ideal in R. We make M into an R-module by defining $rm = \phi(r)m$ for any $r \in R$ and $m \in M$ (and similarly N is an R-module). To see N is a primary R-submodule of M, suppose $r \in R$, $r \neq 0$, $m \in M - N$, and $rm \in N$. Then $\phi(r) \in S$ and $\phi(r)m \in N$, so $\exists t > o$ such that $\phi(r)^t M = \phi(r^t)M \subseteq N$. Thus $r^t M \subseteq N$, and hence N is a primary R-submodule of M. Moreover, $r \in R$ and $r^t M \subseteq N \iff \phi(r^t)M = \phi(r)^t M \subseteq N \iff \phi(r) \in \wp \iff r \in P$, i.e. $\sqrt{Ann_R(M/N)} = P$. □

LEMMA 5.3. *Let N, M, and $A \subseteq R^t$, and suppose N is a primary submodule of M. Then $N \cap A$ is a primary submodule of $M \cap A$.*

PROOF. Let $r \in R$, $m \in (M \cap A) - (N \cap A)$, and suppose $rm \in N \cap A$. Since N is primary, $\exists t > 0$ such that $r^t M \subseteq N$, and hence $r^t(M \cap A) \subseteq N \cap A$. □

DEFINITION 5.4. A submodule N of an R-module M has a *primary decomposition* if $N = \bigcap_{i=1}^{r} Q_i$ with each Q_i a $\wp_i$-primary submodule of M for some prime ideal $\wp_i$ of R . Q_i is called the *primary component of N belonging to $\wp_i$*, and each $\wp_i$ is an *associated prime* of N . If Q_i does not contain $\bigcap_{j \neq i} Q_j$ and the $\wp_i$ are all distinct then the decomposition is said to be *reduced*. Using the fact that the intersection of a finite collection of $\wp$-primary submodules of M is also a $\wp$-primary submodule of M, one sees that if N has a primary decomposition then it has a reduced one. If $\wp_i$ is minimal in the set $\{\wp_1, \ldots, \wp_r\}$ then $\wp_i$ is an *isolated* prime associated to N; otherwise $\wp_i$ is *embedded*.

COROLLARY 5.5. *Let R and S be rings and $\phi : R \to S$ a homomorphism. Let $N \subset M$ be S-modules, and let $N = \cap Q_i$ be a primary decomposition of N as an S-submodule of M with each Q_i a $\wp_i$-primary S-submodule of M. Then $N = \cap Q_i$ is a primary decomposition of N as an R-submodule of M with each Q_i a P_i-primary R-submodule of M, where $P_i = \{r \in R \mid \phi(r) \in \wp_i\}$.*

The following theorem, commonly known as the Lasker-Noether decomposition theorem, tells us for which modules primary decompositions are guaranteed to exist. The standard proof, however, is not constructive.

THEOREM 5.6. *If R is a Noetherian ring with identity and M is an R-module, then any submodule N of M has a reduced primary decomposition.*

PROOF. (See Hungerford, 1974, page 385). □

PROPOSITION 5.7. *If $N = Q_1 \cap Q_2 \cap \cdots \cap Q_r$ and $N = Q'_1 \cap Q'_2 \cap \cdots \cap Q'_s$ are two reduced primary decompositions for $N \subset M$ with each Q_i a $\wp_i$-primary submodule of M and each Q'_j a $\wp'_j$-primary submodule of M then $r = s$ and, with a suitable reordering, $\wp_i = \wp'_i$. Moreover, if $\wp_i$ is isolated then $Q_i = Q'_i$ (with the same reordering).*

PROOF. (See Hungerford, 1974, page 384). □

From Proposition 5.7 we see that primary components of N belonging to isolated primes are unique. The following proposition shows that if every prime associated to N is maximal, then every maximal ideal containing $Ann(M/N)$ has a corresponding primary component in the primary decomposition for N.

PROPOSITION 5.8. *Let N be a submodule of M, and assume $\cap Q_i$ is a primary decomposition for N with each Q_i a $\wp_i$-primary submodule of M . Suppose $\wp_i$ is maximal $\forall i$. If $\wp \subset R$ is a maximal ideal and $Ann(M/N) \subseteq \wp$ then $\exists i$ such that Q_i is $\wp$-primary.*

PROOF. It is easy to see that $\cap Ann(M/Q_i)$ is a (not necessarily reduced) primary decomposition for $Ann(M/N)$. Since $Ann(M/N) = \cap Ann(M/Q_i) \subseteq \wp$, and $\wp$ is prime,

$\sqrt{\cap Ann(M/Q_i)} = \cap \wp_i \subseteq \wp$. Thus $\exists i$ such that $\wp_i \subseteq \wp$. By maximality, $\wp_i = \wp$, hence Q_i is $\wp$-primary. □

6. Gröbner Bases and Dimension

In this section we first review some facts and definitions about the dimensions of ideals and modules, and then show how dimension relates to primary decomposition and the structure of a Gröbner basis. We are able to obtain stronger results when N is viewed as a submodule of $R[X]^s$, rather than as a submodule of some R-module $M \subseteq R[X]^s$, as in Proposition 6.7 and Lemma 6.8. The following definitions and propositions can be found in (Kuntz, 1985; Zariski and Samuel, 1975; Matsumura, 1980).

Recall that the Krull dimension of a ring R, $dim(R)$, is the supremum of the lengths of all chains of prime ideals in R, and if I is and ideal in R then the Krull dimension of I, $dim(I)$, is defined to be $dim(R/I)$. It is easily seen that $\sqrt{I}$ is maximal if and only if $dim(I) = 0$ and I is primary.

DEFINITION 6.1. Let N be an R-module. Then the dimension of N is defined to be $dim(N) = dim(R/Ann(N))$.

Note that this is equivalent to saying $dim(N) = dim(Ann(N))$. Hence the definition of Krull dimension of an ideal I differs from its definition of dimension when viewed as an R-module. Unless otherwise specified, when discussing the dimension of an ideal we will always mean its Krull dimension.

PROPOSITION 6.2. *Suppose $N \subset M$ are R-modules and $dim(M/N) = 0$. Then N is a primary submodule of $M \iff Ann(M/N)$ is a primary ideal of R .*

PROOF. This is a restatement of Lemma 5.1. □

Note that if N is a primary submodule of an R-module M and B is an R-module with $N \subset B \subset M$ then N is also a primary submodule of B. However, this need not be true if $N \subset M \subset B$. For example, let

$$\begin{aligned} N &= \langle (0, x^3), (y - x^2, 0), (x^3 + 1, x), (0, y - x^2) \rangle \\ M &= \langle (0, x), (0, y), (y - x^2, 0), (x^3 + 1, 0) \rangle \\ B &= \mathbf{Q}[x, y]^2 \end{aligned}$$

With the POT ordering on T_2 and the lexicographical ordering on T with $y > x$, the generators given for N and M form Gröbner bases for the modules, respectively. Moreover, $N \subset M \subset B$. Using the computer algebra program CoCoA we determined that

$$\begin{aligned} Ann(M/N) &= \langle y, x^2 \rangle \\ Ann(B/N) &= \langle y - x^2, x^6 + x^3 \rangle \end{aligned}$$

Now $Ann(M/N)$ has radical $\langle y, x \rangle$, which is maximal, hence $Ann(M/N)$ is primary. Thus, N is a primary submodule of M. However, $Ann(B/N)$ is zero-dimensional but not primary, hence N is not a primary submodule of B. Thus, when discussing whether a module N is primary, it is important to be given not only N but the overlying R-module M, as well.

COROLLARY 6.3. *If $A \subseteq N \subset M$ are R-modules, $\wp \subseteq R$ a maximal ideal, and A is a $\wp$-primary submodule of M, then N is also a $\wp$-primary submodule of M.*

PROOF. Since $A \subseteq N$, $Ann(M/A) \subseteq Ann(M/N) \neq R$. Thus, by maximality of $\wp$, $\wp = \sqrt{Ann(M/N)}$. So N is $\wp$-primary in M. □

The situation important to us will be when N and M are R-modules with $N \subset M \subseteq R[X]^s$. Here we recall that $X = \{x_1, \ldots, x_n\}$.

COROLLARY 6.4. *Suppose we have submodules $N \subset M \subseteq R[X]^s$. Let Y be any subset of X, and let $\wp \subseteq R[Y]$ be a maximal ideal. If $Ann(M/N) \cap R[Y]$ is a $\wp$-primary ideal in $R[Y]$, then $N \cap R[Y]^s$ is a $\wp$-primary submodule of $M \cap R[Y]^s$.*

PROOF. Notice that $Ann(M/N) \cap R[Y] \subseteq Ann(M \cap R[Y]^s/N \cap R[Y]^s)$. The result then follows from Proposition 6.2 and Corollary 6.3. □

Being able to decide the primality of ideals in $R[X]$ and determine whether the dimension of an ideal or module is zero is crucial to our work. To do this, however, we need to assume that we already have a primality test for ideals in R and that we can test the irreducibility of univariate polynomials over quotient fields of residue rings of $R[X]$.

LEMMA 6.5. *Let N be an $R[X]$-submodule of $R[x]^s$. Then*

$$Ann_R(R^s/N \cap R^s) = Ann_{R[X]}(R[X]^s/N) \cap R.$$

PROOF. Let $e_1, \ldots, e_s$ be the standard unit basis vectors for R^s (hence also for $R[X]^s$). Then $f \in Ann_R(R^s/N \cap R^s) \iff \forall i\ fe_i \in N \cap R^s \iff f \in R$ *and* $fe_i \in N \forall i \iff f \in Ann_{R[X]}(R[X]^s/N) \cap R$. □

REMARK. Lemma 6.5 is false if we replace R^s by some R-module M containing N. In this case we would want $Ann(M \cap R^s/N \cap R^s) = Ann(M/N) \cap R$. As an example where this is false, we consider ideals in $\mathbf{Q}[x, y, z]$, with $R = \mathbf{Q}[x, y]$ and $s = 1$. Let

$$\begin{aligned} I &= \langle y^2x + yx^2, z^2x + zx^2, z^2y + zy^2, zyx^2 \rangle \\ J &= \langle y^2x + yx^2, z^2x - yx^2, zx^2 + yx^2, zy + zx + yx, yx^3 \rangle. \end{aligned}$$

Using a lexicographical ordering with $z > y > x$, the generators above are Gröbner bases for the ideals, respectively. By Proposition 4.1, we see that

$$\begin{aligned} I \cap R &= \langle y^2x + yx^2 \rangle \\ J \cap R &= \langle y^2x + yx^2, yx^3 \rangle. \end{aligned}$$

Using CoCoA, we computed the following (distinct) ideals:

$$\begin{aligned} Ann(J/I) \cap R &= \langle y^2x + yx^2 \rangle \\ Ann(J \cap R/I \cap R) &= \langle y + x \rangle. \end{aligned}$$

We now prove the analogous results to(Gianni, Trager and Zacharias, 1988, Propositions 5.2 and 5.5) for submodules of free modules. In all that follows we will assume that we are using the lexicographical term order on T with $x_1 > x_2 > \cdots > x_n$, and either the TOP or POT on T_s, and that $\{e_1, \ldots, e_s\}$ is the standard unit basis for $R[X]^s$.

LEMMA 6.6. *Let $N \subseteq R[X]^s$ be a given submodule. If $\Phi \in T_s \cap Lt(N)$ then $\Phi = lt(F)$ for some $F \in N$.*

PROOF. Let $\Omega = G_1, \ldots, G_r$ be a Gröbner basis for N. Write $\Phi = \varphi e_j$ and $lt(G_i) = \varphi_i e_{\sigma(i)}$ for some $\varphi, \varphi_1, \ldots, \varphi_r \in T$. Since $\Phi \in Lt(N)$, $\Phi = \sum_{i=1}^{r} f_i lt(G_i)$ for some $f_1, \ldots, f_r \in R[X]$. Without loss of generality we may assume that for each i either $f_i = 0$ or $f_i = lt(f_i)$. Now

$$\varphi e_j = \Phi = \sum_{i=1}^{r} f_i lt(G_i) = \sum_{i=1}^{r} f_i \varphi_i e_{\sigma(i)} = \sum_{\sigma(i)=j} f_i \varphi_i.$$

Thus if $\sigma(i) = j$ then $lp(f_i)\varphi_i = \varphi$. Let $F = \sum_{\sigma(i)=j} f_i G_i \in N$. Then by construction $\Phi = lt(F)$, as desired. □

PROPOSITION 6.7. *Let $N \subset R[X]^s$ be given, and suppose $dim(R^s/(N \cap R^s)) = 0$. Then $dim(R[X]^s/N) = 0 \iff$ for each $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, s\}$ $\exists\ m_{ij} \geq 0$ such that $x_i^{m_{ij}} e_j \in Lt(N)$.*

PROOF. Let $\Omega = \{G_1, \ldots, G_r\}$ be a Gröbner basis for N . $\Rightarrow$: By assumption, and Lemma 6.5, $dim(Ann(R[X]^s/N)) = dim(Ann(R[X]^s/N) \cap R) = 0$. Hence, by (Gianni, Trager and Zacharias, 1988, Prop. 5.2), $\forall i$, $x_i \in \sqrt{Lt(Ann(R[X]^s/N))}$. So for each $i\ \exists m_i \geq 0$ such that $x_i^{m_i} = lt(f_i)$ for some $f_i \in Ann(R[X]^s/N)$. Using the remark above, we conclude that $\forall i$ and $\forall j$, $x_i^{m_i} e_j = lt(f_i)e_j = lt(f_i e_j) \in Lt(N)$.
$\Leftarrow$: Suppose that for each i and j, $\exists m_{ij} \geq 0$ such that $x_i^{m_{ij}} e_j \in Lt(N)$. Then we have that for each i and j $\exists W_{ij} \in N$ such that $lt(W_{ij}) = x_i^{m_{ij}} e_j$. By (Gianni, Trager and Zacharias, 1988, Prop. 5.2), we only need to show that $x_i \in \sqrt{Lt(Ann(R[X]^s/N))}$ for each i. Fix i. Write $W_{ij} = (g_{1j}, g_{2j}, \ldots, g_{sj})$, and let

$$f_i = \det \begin{vmatrix} W_{i1} & W_{i2} & \cdots & W_{is} \end{vmatrix} = \det \begin{vmatrix} g_{11} & g_{12} & \cdots & g_{1s} \\ \vdots & \vdots & \ddots & \vdots \\ g_{s1} & g_{s2} & \cdots & g_{ss} \end{vmatrix}.$$

Let M_{kj} = the kj-minor of this matrix. Then for $k = 1, \ldots, s$, by expanding along the k^{th} row, we can write

$$f_i = \sum_{j=1}^{s} (-1)^{k+j} g_{kj} M_{kj}.$$

Note that if $r \neq k$ ¡then

$$\begin{aligned} \sum_{j=1}^{s} (-1)^{k+j} g_{kj} M_{kj} &= \pm \text{ the determinant of a matrix with row } r = \text{ row } k \\ &= 0 \end{aligned}$$

and thus

$$\begin{aligned} N \ni \sum_{j=1}^{s} (-1)^{k+j} W_{ij} M_{kj} &= \left(\sum_{j=1}^{s} (-1)^{k+j} g_{1j} M_{kj}, \ldots, \sum_{j=1}^{s} (-1)^{k+j} g_{sj} M_{kj}\right) \\ &= (0, \ldots, f_i, \ldots, 0) \quad f_i \text{ in } k^{th} \text{ coordinate} \\ &= f_i e_k. \end{aligned}$$

Hence $f_i \in Ann(R[X]^s/N)$.

We claim that $lt(f_i) = x_i^{\sum m_{ij}}$. Since $lt(W_{ij}) = x_i^{m_{ij}} e_j$, then $lt(g_{jj}) = x_i^{m_{ij}}$, regardless of the ordering on T_s. Moreover, writing f_i as a polynomial in the g_{jk}'s, the nonzero term $g_{11}g_{22}\cdots g_{ss}$ appears. Using the TOP ordering, $lt(g_{jj}) > lt(g_{kj})\ \forall k < j$ and $lt(g_{jj}) \geq lt(g_{kj})\ \forall k > j$. Thus $lt(f_i) = lt(g_{11}\cdots g_{ss}) = x_i^{\sum m_{ij}}$. Using the POT ordering, for each j, $g_{kj} = 0$ if $k < j$, thus $f_i = \det \begin{vmatrix} g_{11} & 0 & \cdots & 0 \\ g_{21} & g_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{s1} & g_{s2} & \cdots & g_{ss} \end{vmatrix}$, and hence $lt(f_i) = lt(g_{11}\cdots g_{ss}) = x_i^{\sum m_{ij}}$. Thus, using either the POT or TOP ordering, $x_i \in \sqrt{Lt(Ann(R[X]^s/N))}$ for each i. □

Proposition 6.7 is the module analog to(Gianni, Trager and Zacharias, 1988, Prop. 5.2). We would like to find a criteria for determining whether $dim(R[X]^s/N) = 0$ simply by examining a Gröbner basis for N. As in the ideal case, we must make the additional assumption that $N \cap R^s$ is a primary submodule of R^s. Let Ω be a Gröbner basis for N, and set

$$\Omega_{ij} = \{G \in \Omega \mid lt(G) = cx_i^m e_j \text{ for some } c \in R, m \geq 0\}$$

and

$$L_{ij} = \langle c \mid c = lc(G) \text{ for some } G \in \Omega_{ij} \rangle.$$

LEMMA 6.8. *With the above notation, $\exists m$ such that $x_i^m e_j \in Lt(N) \iff L_{ij} = \langle 1 \rangle$.*

PROOF. $\Rightarrow$: Since $x_i^m e_j \in Lt(N) = Lt(\Omega)$, then $x_i^m e_j = \sum_{G\in\Omega} f_G lt(G)$. We can clearly assume that $lt(G) = c_G x_i^{m_G} e_j$ and $f_G = d_G x_i^{m-m_s}$ for all G such that $f_G \neq 0$. Hence $1 = \sum_{G\in\Omega_{ij}} d_G c_G \in L_{ij}$.
$\Leftarrow$: Suppose

$$1 = \sum_{G\in\Omega_{ij}, c_G = lc(G)} \alpha_G c_G \in L_{ij} \text{ for some } \alpha_G \in R.$$

Let $m = \max_{G\in\Omega_{ij}}\{m_G \mid lt(G) = c_G x_i^{m_G} e_j\}$, and for each $G \in \Omega_{ij}$ let $f_G = \alpha_G x_i^{m-m_G}$. Then $x_i^m e_j = \sum_{G\in\Omega_{ij}} f_G lt(G) \in Lt(\Omega_{ij}) \subseteq Lt(N)$. □

We can now prove the module analog of (Gianni, Trager and Zacharias, 1988, Prop. 5.5).

COROLLARY 6.9. *Let $N \subset R[X]^s$ be a given submodule, and Ω be a Gröbner basis for N . Suppose $N \cap R^s$ is a primary submodule of R^s and $dim(R^s/N \cap R^s) = 0$. Then $dim(R[X]^s/N) = 0 \iff$ for each $i = 1,\ldots,n$ and $j = 1,\ldots,s$ $\exists W_{ij} \in \Omega$ such that $lt(W_{ij}) = c_{ij} x_i^{m_{ij}} e_j$ where $m_{ij} \geq 0$ and $c_{ij} \in R$ is a unit modulo $Ann(R[X]^s/N) \cap R$.*

PROOF. Let Ω_{ij} and L_{ij} be as defined in the paragraph preceding Lemma 5.8. We claim that $Ann(R[X]^s/N) \cap R \subseteq L_{ij}$. Indeed, $a \in Ann(R[X]^s/N) \cap R \Rightarrow ae_j \in N$. Thus $ae_j \in Lt(\Omega) \cap Re_j$. So we can write $ae_j = \sum_{G\in\Omega} f_G lt(G)$. We can clearly assume that $lt(G) = c_G e_j$ and $f_G = d_G$ for all G such that $f_G \neq 0$. Hence $a =$

$\sum c_G d_G \in L_{ij}$. Now, since $Ann(R[X]^e/N) \cap R = Ann(R^e/N \cap R^e)$ is zero-dimensional and primary, we have that $\sqrt{Ann(R[X]^e/N) \cap R}$ is maximal. If $L_{ij} \neq \langle 1 \rangle$, then clearly $L_{ij} \subseteq \sqrt{Ann(R[X]^e/N) \cap R}$. Conversely, suppose $L_{ij} \not\subseteq \sqrt{Ann(R[X]^e/N) \cap R}$. Then $\exists a \in L_{ij}$ with $a \notin \sqrt{Ann(R[X]^e/N) \cap R}$. Since $\sqrt{Ann(R[X]^e/N) \cap R}$ is maximal then $\langle a, \sqrt{Ann(R[X]^e/N) \cap R} \rangle = \langle 1 \rangle$. Thus $\exists f \in \sqrt{Ann(R[X]^e/N) \cap R}$ and $b \in R$ such that $1 = f + ab$. Since $Ann(R[X]^e/N) \cap R \subseteq L_{ij}$, $\exists m \geq 0$ such that $f^m \in L$. Thus $1 = 1^m = f^m + a^m b' \in L_{ij}$. Hence we have

$$\begin{aligned} L_{ij} = \langle 1 \rangle &\iff L_{ij} \not\subseteq \sqrt{Ann(R[X]^e/N) \cap R} \\ &\iff \exists W_{ij} \in \Omega_{ij} \text{ such that } lc(W_{ij}) \notin \sqrt{Ann(R[X]^e/N) \cap R} \\ &\iff \langle lc(W_{ij}), Ann(R[X]^e/N) \cap R \rangle = \langle 1 \rangle \\ &\iff lc(W_{ij}) \text{ is a unit modulo } Ann(R[X]^e/N) \cap R. \end{aligned}$$

□

7. Zero-dimensional Case

In this section we present an algorithm for computing the primary decomposition of a module N when it is given as a submodule of some submodule $M \subseteq R[X]^e$ and $dim(M/N) = dim(Ann(M/N) \cap R) = 0$. As in (Gianni, Trager and Zacharias, 1988), not only will we assume that linear equations are solvable in R, but we will also assume that we already have a primality test for ideals in R and that we can test the irreducibility of univariate polynomials over quotient fields of residue rings of $R[X]$. The idea is to compute the primary decomposition of $N \cap R[x_n]^e$, extend that decomposition to a (not necessarily primary) decomposition of N , and proceed by induction on the number of variables to compute a primary decomposition of each component. The algorithm will also give us the associated primes for N, which are unique and maximal. The following theorem describes the induction step.

THEOREM 7.1. *Let $N \subset M \subseteq R[X]^e$, with $dim(M/N) = 0$, and such that $Ann(M/N) \cap R$ is a $\wp$-primary ideal for some maximal ideal $\wp \subset R$. Then we can construct submodules $Q_1, \ldots, Q_r \subseteq M$ and distinct maximal ideals $\wp_1, \ldots, \wp_r \subset R[x_n]$ such that $N = \cap Q_i$ and $Q_i \cap R[x_n]^e$ is a $\wp_i$-primary submodule of $M \cap R[x_n]^e$ for each i.*

PROOF. Let $I = Ann(M/N) \cap R[x_n]$. Since $dim(Ann(M/N)) = dim(Ann(M/N) \cap R) = 0$, then $dim(I) = 0$. Thus, by (Gianni, Trager and Zacharias, 1988, Prop. 5.7) we can compute a $g \in I$ such that $\sqrt{I} = \sqrt{\langle g, \wp \rangle}$. Let $g(x_n) \equiv \prod_{i=1}^{r} p_i(x_n)^{t_i} \bmod \wp$ be the complete factorization of g mod $\wp$, i.e. the images of $p_i(x_n)$ in $(R/\wp)[x_n]$ are pairwise relatively prime irreducible non-units. Since $\prod p_i^{t_i} \in \sqrt{I}$, $\exists t$ such that $\prod p_i^{t_i t} \in I$. Note that t is computable since ideal membership is decidable. For each $i = 1, \ldots, r$ let

$$Q_i = p_i^{t_i t} M + N$$

and

$$\wp_i = \langle p_i, \wp \rangle R[x_n].$$

Since p_i is irreducible modulo $\wp$, $\wp_i$ is a maximal ideal in $R[x_n]$. Clearly the $\wp_i$ are distinct.

Claim 1: $N = \bigcap_{i=1}^{r} Q_i$.
Since R is Noetherian and $Ann(M/N) \cap R$ is $\wp$-primary then $\exists m > 0$ such that $\wp^m \subseteq Ann(M/N) \cap R \subseteq Ann(M/N)$. For any $i \neq j$, p_i and p_j are comaximal modulo $\wp$, i.e. $\langle p_i \rangle + \langle p_j \rangle \equiv \langle 1 \rangle \bmod \wp$. Hence $\exists a, b \in R$ and $\alpha \in \wp$ such that $ap_i + bp_j + \alpha = 1$. Now $\alpha^m \in Ann(M/N)$, so $1 = 1^m = (ap_i + bp_j + \alpha)^m = a'p_i + b'p_j + \alpha^m$ with $a', b' \in R$. Thus p_i and p_j are comaximal modulo $Ann(M/N)$. A similar argument then shows $p_i^{t_i t}$ and $p_j^{t_j t}$ are also comaximal modulo $Ann(M/N)$. Thus we have $(\langle p_i^{t_i t} \rangle M + N) \cap (\langle p_j^{t_j t} \rangle M + N) = \langle p_i^{t_i t} p_j^{t_j t} \rangle M + N$. By induction on r, and the fact that for any i, $p_i^{t_i t}$ and $\prod_{j \neq i} p_j^{t_j t}$ are also comaximal modulo $Ann(M/N)$, we have

$$\bigcap_{i=1}^{r} Q_i = \bigcap_{i=1}^{r} (\langle p_i^{t_i t} \rangle M + N) = \langle \prod_{i=1}^{r} p_i^{t_i t} \rangle M + N = N.$$

Claim 2: $Q_i \cap R[x_n]^s$ is a $\wp_i$-primary submodule of $M \cap R[x_n]^s$.
Let $I_i = \langle p_i^{t_i t}, Ann(M/N) \rangle$. Recall that we have $\wp^m \subseteq Ann(M/N) \cap R$ for some $m > 0$. If $\alpha_i = \max\{t_i t, m\}$ then $\wp_i^{\alpha_i} \subseteq I_i \cap R[x_n]$, and hence either $I_i \cap R[x_n]$ is $\wp_i$-primary or it is the unit ideal. Suppose $I_i \cap R[x_n] = \langle 1 \rangle$, hence $I_i = \langle 1 \rangle$. Then, since $\prod_{j \neq i} p_j^{t_j t} I_i \subseteq Ann(M/N)$, we have $\prod_{j \neq i} p_j \in \sqrt{Ann(M/N) \cap R[x_n]} = \sqrt{I} = \sqrt{\langle g, \wp \rangle}$, and so $\prod_{j \neq i} p_j^{\alpha} \in \langle g, \wp \rangle$ for some $\alpha > 0$. By the comaximality modulo $\wp$ of p_i and $\prod_{j \neq i} p_j^{\alpha}$ we have that for some $f, h \in R[x_n]$, $1 \equiv f p_i + h \prod_{j \neq i} p_j^{\alpha} \bmod \wp$. Writing $\prod_{j \neq i} p_j^{\alpha} = wg + a$ for some $w \in R[x_n]$ and $a \in \wp$, we then have

$$1 \equiv \; fp_i + hwg \;\bmod \wp \equiv \; p_i (f + hwp_i^{t_i t - 1} \prod_{j \neq i} p_j^{t_j t}) \;\bmod \wp,$$

i.e. p_i is a unit modulo $\wp$. This is a contradiction. Hence $I_i \cap R[x_n]$ is $\wp_i$-primary. Moreover, since $f \in I_i$, then $f = p_i^{t_i t} q + b$ for some $q \in R[X]$, $b \in Ann(M/N)$. Thus, $fv = p_i^{t_i t} qv + bv \in Q_i \; \forall v \in M$, i.e. $f \in Ann(M/Q_i)$. So $I_i \cap R[x_n] \subseteq Ann(M/Q_i) \cap R[x_n]$, and hence $Ann(M/Q_i) \cap R[x_n]$ is $\wp_i$-primary. (Note that by Proposition 5.8, $Q_i \subset M$.) Thus, by Corollary 6.5, $Q_i \cap R[x_n]^s$ is a $\wp_i$-primary submodule of $M \cap R[x_n]^s$. □

We note that since $Ann(M/N) \subseteq Ann(M/Q_i)$ and $dim(M/N) = 0$, then $dim(M/Q_i) = 0$. Thus we may recursively apply the theorem to Q_i and $\wp_i$ over the base ring $R[x_n]$ and hence compute the primary decomposition of N and its associated primes.

COROLLARY 7.2. *If N is a submodule of $R[X]^s$, $dim(R[X]^s/N) = 0$, and $N \cap R^s$ is a $\wp$-primary submodule of R^s for some maximal ideal $\wp \subset R$, then we can construct submodules $Q_1, \ldots, Q_r \subseteq R[X]^s$ and maximal ideals $\wp_1, \ldots, \wp_r \subset R[x_n]$ such that $N = \cap Q_i$ and $Q_i \cap R[x_n]^s$ is a $\wp_i$-primary submodule of $R[x_n]^s$ for each i.*

PROOF. By Lemma 6.5, $Ann(R[X]^s/N) \cap R$ is $\wp$-primary if and only if $N \cap R^s$ is a $\wp$-primary submodule of R^s. Thus we may apply Theorem 7.1 with $M = R[X]^s$. □

Algorithm MZPD $(R; X; N; M; \wp)$ *Zero-dimensional primary decomposition*
Input: R, a ring; $X = x_1, \ldots, x_n$, indeterminates; $N \subset M$, submodules of $R[X]^s$; $\wp$, a maximal ideal of R
where: $N \cap R^s$ is a $\wp$-primary submodule of $M \cap R^s$, and $dim(M/N) = 0$
Output: $\{(Q_1, \wp_1), \ldots, (Q_r, \wp_r)\}$

where: $\wp_i$ is a maximal ideal of $R[X]$, Q_i is a $\wp_i$-primary submodule of M, $\wp_i \neq \wp_j$ $\forall i \neq j$, and $N = \cap_{i=1}^{r} Q_i$.

Begin

If $n = 0$ then return $\{(N, \wp)\}$

Else Compute $Ann(M/N)$

Compute a minimal Gröbner basisΩ for $Ann(M/N) \cap R[x_n]$

Select $g \in \Omega$ of largest degree

Compute the complete factorization of g mod $\wp$,

$$g = \prod_{i=1}^{m} p_i^{t_i} \text{ in } (R/\wp)[x_n], \quad p_i \in R[x_n].$$

Find t such that $\prod p_i^{t_i t} \in Ann(M/N) \cap R[x_n]$

Set $Q_i = p_i^{t_i t} M + N$ for $i = 1, \ldots, m$

Set $\wp_i = \langle p_i, \wp \rangle R[x_n]$ for $i = 1, \ldots, m$

Return $\cup_i MZPD(R[x_n]; x_1, \ldots, x_{n-1}; Q_i; M; \wp_i)$.

8. Primary Decomposition over a Principle Ideal Domain

We now want to consider cases where $dim(M/N)$ is not zero. To do this, however, we need to restrict our ring R to one which is also a Principal Ideal Domain (PID).

LEMMA 8.1. *Let R be a PID, $p \in R$ prime, and $J \subseteq R[x]$ an ideal. (Here x is a single indeterminate.) Suppose $J \cap R$ is pR-primary and $J \not\subseteq pR[x]$. Then either $J = R[x]$ or $dim(J) = 0$.*

PROOF. Suppose $J \neq R[x]$. Then $\exists \wp \subset R[x]$, a prime ideal containing J. Since $J \not\subseteq pR[x]$ then $\exists g \in \wp - pR[X]$. Moreover, we can choose g to be irreducible modulo p. Since $J \cap R \subseteq \wp \cap R$, and the latter is a prime ideal of R, then $pR = \sqrt{J \cap R} \subseteq \wp \cap R$. Hence $\langle p, g \rangle R[X] \subseteq \wp$. Since $\langle p, g \rangle R[X]$ is maximal, $\wp$ is maximal, thus $dim(J) = 0$. □

LEMMA 8.2. *Let R be an integral domain, N a given submodule of $R[X]^s$, $\langle p \rangle \subset R$ a principal prime ideal. Then it is possible to find $g \in R - \langle p \rangle$ such that*

$$N = (N + gR[X]^s) \cap (NR_{\langle p \rangle}[X] \cap R[X]^s).$$

PROOF. By Proposition 4.6 we can find $a \in R - \langle p \rangle$ such that

$$NR_{\langle p \rangle}[X] \cap R[X]^s = NR_a[X] \cap R[X]^s.$$

Since $R[X]^s$ is Noetherian, $\exists m \geq 0$ such that $a^m(NR_{\langle p \rangle}[X] \cap R[X]^s) \subseteq N$. Note that given a basis for $NR_a[X] \cap R[X]^s$, m is computable. Let $g = a^m$. Clearly, $N \subseteq (N + gR[X]^s) \cap (NR_{\langle p \rangle}[X] \cap R[X]^s)$. To show the reverse containment, suppose $F \in (N + gR[X]^s) \cap (NR_{\langle p \rangle}[X] \cap R[X]^s)$. Then we can write $F = w + gv$, where $w \in N$ and $v \in R[X]^s$. Now $gF \in N$, so $g^2 v \in N$. Hence $v \in NR_a[X] \cap R[X]^s$, and $gv \in N$. Thus $F \in N$. □

COROLLARY 8.3. *Let R be an integral domain, $N \subset M$ submodules of $R[X]^s$, $\langle p \rangle \subset R$ a principal prime ideal. Denote $N^{ec} := NR_{\langle p \rangle}[X] \cap M$. Then it is possible to find $g \in R - \langle p \rangle$ such that*

$$N = (N + gM) \cap N^{ec}.$$

PROOF. By Lemma 8.2 we can find $g \in R - \langle p \rangle$ such that $N = (N + gR[X]^s) \cap (NR_{\langle p \rangle}[X] \cap R[X]^s)$. Since $M \subseteq R[X]^s$, intersecting both sides of this equation with M gives $N = (N + gR[X]^s) \cap N^{ec}$. Now

$$\begin{aligned} N \subset M \subseteq R[X]^s &\Rightarrow N + gM \subseteq N + gR[X]^s \\ &\Rightarrow N \subseteq (N + gM) \cap N^{ec} \subseteq (N + gR[X]^s) \cap N^{ec} = N \\ &\Rightarrow N = (N + gM) \cap N^{ec}. \end{aligned}$$

□

LEMMA 8.4. *Let R be a PID. Let $N \subset M$ be submodules of $R[X]^s$. Assume $Ann(M/N) \cap R$ is $\langle p \rangle$-primary for some maximal ideal $\langle p \rangle \subset R$. Then we can compute a primary decomposition for N in M.*

PROOF. If $dim(Ann(M/N)) = 0$, use MZPD to decompose N . Otherwise, by (Gianni, Trager and Zacharias, 1988, Cor. 5.4), we can find i such that $dim(Ann(M/N) \cap R[x_i]) \neq 0$. Let $\wp = pR[x_i]$. By Corollary 8.3 we can find $g \in R[x_i] - \wp$ such that $N = (N + gM) \cap N^{ec}$ where $N^{ec} = N(R[x_i])_\wp[X'] \cap M$ and $X' = x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$.
Claim: $N \subset N + gM$
If $gM \subseteq N$ then $g \in Ann(M/N) \cap (R[x_i] - \wp)$. Thus $Ann(M/N) \cap R[x_i]$ contains both the pR-primary ideal $Ann(M/N) \cap R$ and the element $g \notin \wp$. Hence, by Lemma 8.1, either $Ann(M/N) \cap R[x_i]$ is zero-dimensional (which we have assumed it isn't) or is the unit ideal (which forces $N = M$, another contradiction). Thus $N \neq N + gM$. Write $N' = N + gM$, and suppose $N' \neq M$ and $dim(Ann(M/N') \cap R[x_i]) \neq 0$. Since $Ann(M/N) \cap R \subseteq Ann(M/N') \cap R$, $Ann(M/N') \cap R$ is also pR-primary. Thus, as before with N, we can find $h \in R[x_i] - \wp$ such that $N' = (N' + hM) \cap (N')^{ec}$, where $(N')^{ec} = N'R[x_i]_\wp[X'] \cap M$. Again by the claim, $h \notin Ann(M/N')$. Now,

$$\begin{aligned} N = N' \cap N^{ec} &= (N' + hM) \cap (N')^{ec} \cap N^{ec} \\ &= (N + gM + hM) \cap (N')^{ec} \cap N^{ec} \\ &= (N + \langle g, h \rangle M) \cap N^{ec}. \end{aligned}$$

Again we must consider the possibility that we have both $(N + \langle g, h \rangle M) \neq M$ and $dim(Ann(M/N + \langle g, h \rangle M) \cap R[x_i]) \neq 0$. Since $R[X]^s$ is Noetherian, continuing this way we will eventually end up with a finite set $F \subseteq R[x_i] - \langle p \rangle R[x_i]$ such that $N = (N + FM) \cap N^{ec}$ and either $N + FM = M$ or $dim(Ann(M/N + FM) \cap R[x_i]) = 0$. Thus it is sufficient to decompose $N + FM$ and N^{ec} separately.

First we decompose $N + FM$. Case 1: Suppose $dim(Ann(M/N + FM) \cap R[x_i]) = 0$. If $dim(Ann(M/N + FM)) = 0$, then, since $Ann(M/N + FM) \cap R \supset Ann(M/N) \cap R$ is also $\langle p \rangle$-primary, we can use MZPD to decompose $N + FM$. Otherwise, $\exists j \neq i$ such that $dim(Ann(M/N + FM) \cap R[x_j]) \neq 0$. Hence we can compute a finite set H containing F such that $N = (N + HM) \cap N^{ec}$ where now $N^{ec} = NR[x_j]_{pR[x_j]}[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n]$ and either $N + HM = M$ or $dim(M/N + HM) \cap R[x_j] = 0$. Thus, we can compute the primary decomposition of $N + FM$ by inducting on the number of variables x_j such that

$dim(Ann(M/N+FM)\cap R[x_j]) \neq 0$. Case 2: Suppose $dim(Ann(M/N)+FM)) \neq 0$, i.e. $N+FM = M$. Then $N = N^{ec}$. Thus it remains to decompose N^{ec}. Let $N^e = NR[x_i]_p[X']$ and $M^e = MR[x_i]_p[X']$. Note that if $N^e = M^e$ then $M \subseteq MR[x_i]_p[X'] \cap M = M^{ec} = N^{ec} \subseteq M$, hence $N^{ec} = M$ and $N = N+FM \neq M$. Thus we assume $N^e \neq M^e$. To decompose $N^{ec} \subset M^{ec}$, it is enough to decompose N^e as an $R[x_i]_p[X']$-submodule of M^e and contract the results via Corollary 4.2. This gives us a primary decomposition of N^{ec} as an $R[X]$-submodule of M^{ec}. Note that $R[x_i]_p$ is also a PID and p_p is a maximal ideal. We now show that $Ann(M/N)R[x_i]_p[X'] \cap R[x_i]_p$ is p_p–primary. Since $Ann(M/N) \cap R$ is pR-primary, and pR is maximal, then $\exists \alpha > 0$ such that $p^\alpha \in Ann(M/N)$, hence $p^\alpha \in Ann(M/N)R[x_i]_p[X']$. Recall that we were able to assume at the beginning that $dim(Ann(M/N) \cap R[x_i] \neq 0$. Let P be a non-zero dimensional associated prime of $Ann(M/N) \cap R[x_i]$. Then, since $p^\alpha \in Ann(M/N) \cap R[x_i] \subseteq P$, we have $p \subseteq P$. Since p is one-dimensional, $P = p$ and hence $Ann(M/N) \cap R[x_i] \subseteq p$. Now we have $p^\alpha \in Ann(M/N)R[x_i]_p[X'] \cap R[x_i]_p \subseteq p_p$, and p_p is maximal. So $Ann(M/N)R[x_i]p[X'] \cap R[x_i]_p$ is p_p-primary. Since

$$Ann(M/N)R[x_i]_p[X'] \cap R[x_i]_p \subseteq Ann(M^e/N^e) \cap R[x_i]_p,$$

the right hand side is also p_p-primary. Since $R[x_i]_p$ is a PID, $Ann(M^e/N^e) \cap R[x_i]_p$ is p_p-primary, and p_p is maximal, then $N^e \subset M^e \subseteq R[x_i]_p[X']^s$ satisfies the hypotheses of the theorem. We therefore may induct on the number of variables n to compute a primary decomposition of N^e. □

THEOREM 8.5. *Let R be a PID, and let $N \subset M$ be submodules of $R[X]^s$. Then we can compute the primary decomposition for N in M.*

PROOF. Suppose $dim(Ann(M/N) \cap R) \neq 0$. In this case, $Ann(M/N) \cap R = \langle 0 \rangle$ and R is not a field. Then, by Corollary 8.3, we can find $a \in R - \langle 0 \rangle$ such that $N = (N+aM) \cap N^{ec}$ where $N^{ec} = NR_{\langle 0 \rangle}[X] \cap M$. Moreover, $N \neq N+aM$, as was shown in the proof of Lemma 8.4. Once again, we can decompose N^{ec} and $N+aM$ separately. Since $R_{\langle 0 \rangle}$ is a field, we can apply Lemma 8.4 to $NR_{\langle 0 \rangle}[X] \subset MR_{\langle 0 \rangle}[X]$, submodules of $R_{\langle 0 \rangle}[X]^s$, to compute a primary decomposition for $NR_{\langle 0 \rangle}[X]$, and the results can be contracted to M. Thus it remains to decompose $N+aM$. But, since $a \in Ann(M/N+aM) \cap R$, then $dim(Ann(M/N+aM) \cap R) = 0$.

Thus we have reduced to the case where $dim(Ann(M/N) \cap R) = 0$. So, assuming $dim(Ann(M/N) \cap R) = 0$, write $Ann(M/N) \cap R = \langle \prod_{i=1}^t p_i^{m_i} \rangle$ where $p_i \in R$ is prime. Let $N_i = N + p_i^{m_i} M$ for $i = 1, \ldots, t$. Then we have $p_i^{m_i} \in Ann(M/N_i) \cap R$ and $Ann(M/N_i) \cap R \subseteq p_i R$, thus $Ann(M/N_i) \cap R$ is a $p_i R$-primary ideal. Hence $N_i \subset M$ can be decomposed by Lemma 8.4.

Claim: $N = \cap N_i$.

$\subseteq$: Clear.

$\supseteq$: Let $f \in \cap N_i$. Then for each i $\exists u_i \in N$ and $\exists v_i \in M$ such that $f = u_i + p_i^{m_i} v_i$. Let $s = \prod p_i^{m_i}$, and for each i let $q_i = \frac{s}{p_i^{m_i}}$. Since the p_i are distinct primes, $\exists r_1, \ldots, r_t$ such that $\sum r_i q_i = 1$. Thus

$$f = \sum r_i q_i f = \sum r_i q_i (u_i + p_i^{m_i} v_i) = \sum r_i q_i u_i + \sum r_i s v_i \in N.$$

By taking the intersection of the decompositions for each N_i we obtain a decomposition for N. □

We now give the algorithms corresponding to Lemma 8.4 and Theorem 8.5.

Algorithm MPDC$(R; X; N; M; p)$ *Primary decomposition over a PID, primary contraction case*

Input: R, a ring; $X = x_1, \ldots, x_n$, indeterminates; $N \subset M$ submodules of $R[X]^s$; p, a prime element of R

where: $Ann(M/N) \cap R$ is pR-primary

Output: $\{Q_1, \ldots, Q_r\}$ a primary decomposition for N in M.

Begin

If $dim(Ann(M/N)) = 0$ then Return MZPD$(R; X; N; M; \langle p \rangle)$

Else Find i such that$dim(Ann(M/N) \cap R[x_i] \neq 0$

Set $\wp := pR[x_i]$

Set $X' := x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$

Set $N^{ec} := NR[x_i]_{\wp}[X] \cap M$

Set $N' := N$

Repeat

Find $g \in R[x_i] - \wp$ such that $N = (N + gM) \cap N^{ec}$

Set $N' := N + gM$

Until either $N' = M$ or $dim(Ann(M/N') \cap R[x_i]) = 0$

Set $\{Q_1, \ldots, Q_m\} :=$ MPDC$(R[x_i]_{(p)}; X'; NR[x_i]_{\wp}[X']; MR[x_i]_{\wp}[X']; \wp_{\wp})$

Set $Q_i^c := Q_i \cap M$ for $i = 1, \ldots, m$

If $N' = M$ then Return $\{Q_1^c, \ldots, Q_m^c\}$

Else Set $\{Q_{m+1}, \ldots, Q_r\} :=$ MPDC$(R; X; N'; M; p)$

Return $\{Q_1^c, \ldots, Q_m^c, Q_{m+1}, \ldots, Q_r\}$.

Algorithm MPD$(R; X; N; M)$ *Primary decomposition over a PID*

Input: R, a ring; $X = x_1, \ldots, x_n$, indeterminates; $N \subset M$ submodules of $R[X]^s$

Output: $\{Q_1, \ldots, Q_r\}$ a primary decomposition for N

Begin

Set $N^{ec} := NR_{(0)}[X] \cap M$

Set $N' := N$

If $dim(Ann(M/N) \cap R \neq 0$

Then Find $a \in R - \langle 0 \rangle$ such that $N = (N + aM) \cap N^{ec}$

Set $\{Q_1, \ldots, Q_m\} :=$ MPDC$(R_{(0)}[X]; X; NR_{(0)}[X]; MR_{(0)}[X])$

Set $Q_i^c := Q_i \cap M$ for $i = 1, \ldots, m$

Set $N' := N + aM$

Else Set $N' := N$

Write $Ann(M/N') \cap R = \langle \prod_{i=1}^{t} p_i^{m_i} \rangle$ with p_i irreducible

Set $N_i := N' + p_i^{m_i} M$ for $i = 1, \ldots, t$

Set $\{Q_{m+1}, \ldots, Q_r\} := \cup_i$ MPDC$(R; X; N_i; M; \langle p_i \rangle$

Return $\{Q_1^c, \ldots, Q_m^c, Q_{m+1}, \ldots, Q_r\}$.

References

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: (Bose, N.K., ed.)*Multidimensional Systems Theory*, D. Reidel Publishing Co., pp. 184-232.

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. of Symb. Comp.* **16**, 149-167.

Hungerford, T. (1974). *Algebra.* Graduate Texts in Mathematics Volume 73. Springer-Verlag, New York.

Kuntz, E. (1985). *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, Boston.

Lazard, D. (1985). Ideal bases and primary decomposition: case of two variables. *J. of Symb. Comp.* **1**, 261-270.

Matsumura, H. (1980). *Commutative Algebra* second edition. The Benjamin/Cummings Publ. Company.

Möller, H. M. (1988). On the construction of Gröbner bases using syzygies. *J. of Symb. Comp.* **6**, 345-359.

Möller, H. M., Mora, F. (1986). New constructive methods in classical ideal theory. *J. Algebra* **100**, 133-178.

Rutman, E. W. (1992). Computing primary decompositions of modules. *Ph.D. Thesis, University of Maryland.*

Zariski, O., Samuel, P. (1975). *Commutative Algebra, Volume I.* Graduate Texts in Mathematics Volume 28. Springer-Verlag, Heidelberg.